Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1   1.   (currently amended): A system for dynamically identifying internal
2   hosts in a heterogeneous computing environment with multiple subnetworks,
3   comprising:
4   an analysis module analyzing a plurality of packets, each such packet
5   comprising a source address of an originating host and a destination address of a
6   receiving host; and
7   a classification module classifying an unknown originating host located at
8   the source address of an outbound packet as an inside host with high confidence,
9   classifying an unknown receiving host located at the destination address of an
10   inbound packet as an inside host, [[and]] reclassifying the unknown receiving host
11   as an inside host with high confidence upon receiving a further outbound packet
12   having a source address corresponding to the address of the unknown receiving
13   host, managing packet traffic flow by monitoring the packets and adjusting
14   control flow thereof, and ignoring packet traffic flow for each packet with an
15   originating host or a receiving host classified as an inside host with high
16   confidence.

1   2.   (original): A system according to Claim 1, further comprising:
2   the classification module further classifying an unknown originating host
3   located at the source address of an inbound packet as an outside host.

1   3.   (original): A system according to Claim 2, further comprising:
2   the classification module reclassifying the unknown originating host as an
3   inside host with high confidence upon receiving an outbound packet having a
4   source address corresponding to the address of the unknown originating host.

1   4.   (original): A system according to Claim 1, further comprising:

-2-

2   the classification module further classifying an unknown receiving host

3 located at the destination address of an outbound packet as an outside host.

1   5. (original): A system according to Claim 4, further comprising:

2   the classification module reclassifying the unknown receiving host as an

3 inside host with high confidence upon receiving an inbound packet having a

4 destination address corresponding to the address of the unknown receiving host.

1   6. (original): A system according to Claim 1, further comprising:

2   the classification module maintaining the inside host with high confidence

3 classification of the unknown originating host upon receiving at least one of

4 further inbound packets and further outbound packets.

1   7. (original): A system according to Claim 1, further comprising:

2   the classification module maintaining the inside host with high confidence

3 classification of the unknown receiving host upon receiving at least one of further

4 inbound packets and further outbound packets.

1   Claim 8 (canceled).

1   Claim 9 (canceled).

1   10. (original): A system according to Claim 1, wherein the packets are

2 communicated via a point-to-point protocol.

1   11. (original): A system according to Claim 1, wherein the packets are

2 communicated via an end-to-end protocol.

1   12. (original): A system according to Claim 1, wherein the packets are

2 communicated via the TCP/IP protocol and each source address and destination

3 address is an internet protocol (IP) address.

1   13. (currently amended): A method for dynamically identifying

2 internal hosts in a heterogeneous computing environment with multiple

3 subnetworks, comprising:

-3-

4   analyzing a plurality of packets, each such packet comprising a source

5   address of an originating host and a destination address of a receiving host;

6   classifying an unknown originating host located at the source address of

7   an outbound packet as an inside host with high confidence;

8   classifying an unknown receiving host located at the destination address of

9   an inbound packet as an inside host; [[and]]

10   reclassifying the unknown receiving host as an inside host with high

11   confidence upon receiving a further outbound packet having a source address

12   corresponding to the address of the unknown receiving host;

13   managing packet traffic flow by monitoring the packets and adjusting

14   control flow thereof; and

15   ignoring packet traffic flow for each packet with an originating host or a

16   receiving host classified as an inside host with high confidence.

1   14.   (original): A method according to Claim 13, further comprising:

2   classifying an unknown originating host located at the source address of

3   an inbound packet as an outside host.

1   15.   (original): A method according to Claim 14, further comprising:

2   reclassifying the unknown originating host as an inside host with high

3   confidence upon receiving an outbound packet having a source address

4   corresponding to the address of the unknown originating host.

1   16.   (original): A method according to Claim 13, further comprising:

2   classifying an unknown receiving host located at the destination address of

3   an outbound packet as an outside host.

1   17.   (original): A method according to Claim 16, further comprising:

2   reclassifying the unknown receiving host as an inside host with high

3   confidence upon receiving an inbound packet having a destination address

4   corresponding to the address of the unknown receiving host.

1   18.   (original): A method according to Claim 13, further comprising:

-4-

2   maintaining the inside host with high confidence classification of the
3 unknown originating host upon receiving at least one of further inbound packets
4 and further outbound packets.

1   19.   (original): A method according to Claim 13, further comprising:
2   maintaining the inside host with high confidence classification of the
3 unknown receiving host upon receiving at least one of further inbound packets
4 and further outbound packets.

1   Claim 20 (canceled).

1   Claim 21 (canceled).

1   22.   (original): A method according to Claim 13, wherein the packets
2 are communicated via a point-to-point protocol.

1   23.   (original): A method according to Claim 13, wherein the packets
2 are communicated via an end-to-end protocol.

1   24.   (original): A method according to Claim 13, wherein the packets
2 are communicated via the TCP/IP protocol and each source address and
3 destination address is an internet protocol (IP) address.

1   25.   (currently amended): A computer-readable storage medium
2 holding code for performing the method according to Claims 13, 14, 15, 16, 17,
3 18, ~~19, 20 and 21~~ and 19.

1   26.   (currently amended): A system for classifying hosts in a
2 heterogeneous computing environment, comprising:
3   a table storing records comprising a plurality of states which each specify
4 a location of a host relative to a network domain boundary, the states comprising:
5   an *Unknown* state describing an undefined host;
6   an *Outside* state describing a host located outside the network
7 domain boundary;

-5-

8   an *Inside* state describing a host provisionally located inside the

9   network domain boundary; and

10   an *Inside with High Confidence* state describing a host located

11   inside the network domain boundary;

12   a traffic manager classifying the hosts based on source address with each

13   outbound packet originating from an *Unknown* state, *Outside* state or *Inside* state

14   into an *Inside with High Confidence* ~~state and~~ state, classifying the hosts based on

15   destination address with each inbound packet originating from an *Unknown* state

16   or *Outside* state into an *Inside with High Confidence* state, classifying the hosts

17   based on source address with each inbound packet originating from an *Unknown*

18   state into an *Outside* state, classifying the hosts based on destination address with

19   each outbound packet originating from an *Unknown* state into an *Outside* state,

20   and ignoring packet traffic based on source address or destination address with

21   each outbound packet and each inbound packet originating from an *Inside with*

22   *High Confidence* state.

1   Claim 27 (canceled).

1   28.   (original): A system according to Claim 26, further comprising:

2   the traffic manager passing through packet traffic based on source address

3   with each inbound packet originating from an *Outside* state, *Inside* state or *Inside*

4   *with High Confidence* state and with each outbound packet originating from an

5   *Inside with High Confidence* state.

1   Claim 29 (canceled).

1   30.   (original): A system according to Claim 26, further comprising:

2   the traffic manager passing through packet traffic based on destination

3   address with each outbound packet originating from an *Outside* state, *Inside* state

4   or *Inside with High Confidence* state and with each inbound packet originating

5   from an *Inside with High Confidence* state.

1   Claim 31 (canceled).

-6-

1   32.   (original): A system according to Claim 26, wherein the

2 heterogeneous computing environment is IP compliant.

3   33.   (currently amended): A method for classifying hosts in a

4 heterogeneous computing environment, comprising:

5   defining a plurality of states which each specify a location of a host

6 relative to a network domain boundary, the states comprising:

7   an *Unknown* state describing an undefined host;

8   an *Outside* state describing a host located outside the network

9 domain boundary;

10   an *Inside* state describing a host provisionally located inside the

11 network domain boundary; and

12   an *Inside with High Confidence* state describing a host located

13 inside the network domain boundary;

14   classifying the hosts based on source address with each outbound packet

15 originating from an *Unknown* state, *Outside* state or *Inside* state into an *Inside*

16 *with High Confidence* state; [[and]]

17   classifying the hosts based on destination address with each inbound

18 packet originating from an *Unknown* state or *Outside* state into an *Inside with*

19 *High Confidence* state;

20   classifying the hosts based on source address with each inbound packet

21 originating from an *Unknown* state into an *Outside* state;

22   classifying the hosts based on destination address with each outbound

23 packet originating from an *Unknown* state into an *Outside* state; and

24   ignoring packet traffic based on source address or destination address with

25 each outbound packet and each inbound packet originating from an *Inside with*

26 *High Confidence* state.

1 Claim 34 (canceled).

1   35.   (original): A method according to Claim 33, further comprising:

-7-

2   passing through packet traffic based on source address with each inbound

3 packet originating from an *Outside* state, *Inside* state or *Inside with High*

4 *Confidence* state and with each outbound packet originating from an *Inside with*

5 *High Confidence* state.

1   Claim 36 (canceled).

1   37.   (original): A method according to Claim 33, further comprising:

2   passing through packet traffic based on destination address with each

3 outbound packet originating from an *Outside* state, *Inside* state or *Inside with*

4 *High Confidence* state and with each inbound packet originating from an *Inside*

5 *with High Confidence* state.

1   Claim 38 (canceled).

1   39.   (original): A method according to Claim 33, wherein the

2 heterogeneous computing environment is IP compliant.

1   40.   (currently amended): A computer-readable storage medium

2 holding code for performing the method according to Claims 33, [[34,]] 35, [[36]]

3 and 37.

-8-